CITRIX PRESENTATION SERVER 4.0 FOR WINDOWS

Product Description

The Citrix Presentation Server 4.0 for Windows (henceforth referred to as the Citrix PS) is a remote access/application publishing product that provides users with secure access to applications and information available from central servers. This access can be from a range of devices over any network connection including Internet, LAN, WAN, dial-up or wireless connection.

Clients access applications published on the server side by logging on through a web browser. Data sent between the Client and Application Server is encrypted using a secure https connection. The Citrix PS does not implement encryption itself - all encryption is provided by Windows SSL/TLS encryption functions. The highest level of available encryption is 168-bit 3DES.

Scope of Evaluation

The scope of the Common Criteria (CC) certification included the following security functionality:

- Cryptographic Key Management
- Cryptographic Operation
- Internal Data Transfer Protection
- Identification and Authentication
- Domain Separation

Common Criteria Certification Summary

The product has met the requirement of the Common Criteria (CC) evaluation assurance to EAL 2.

DSD's Cryptographic Evaluation

Because the product employs cryptography, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria certification.

Due to the fact that the Citrix PS is reliant on the underlying operating system (Windows Server 2003) to implement end-to-end encryption, the approval of the Citrix PS for Australian Government use is contingent upon Server 2003 successfully completing a DSD cryptographic evaluation. At the time of writing the DSD cryptographic evaluation of Server 2003 is still in progress.

DSD's Recommendations

It is possible to configure Server 2003 to employ encryption algorithms that have not been approved for Australian Government use. Therefore, in order to configure Server 2003 appropriately, Australian Government users of the Citrix PS are instructed to enable the System cryptography: Use FIPS compliant algorithms for encryption option in the Local Security Policy security settings on Server 2003. This ensures that 3DES encryption is used for secure https connections. For more information regarding DSD Approved Cryptographic Algorithms (DACAs) please see ACSI 33 Chapter 9 on Cryptography.

The product has been evaluated to EAL 2. As such, the Citrix PS can be used to transmit:

- UNCLASSIFIED data over networks of any classification
- IN-CONFIDENCE data over networks of any classification

Should Windows Server 2003 pass cryptographic evaluation by DSD, the consumer guide will be re-written to reflect this outcome.

It should be noted that information classified CONFIDENTIAL, SECRET or TOP SECRET MUST be encrypted using High Grade Cryptographic Equipment if it is transmitted over a network of lower classification.

Point of Contact

For further information regarding the certification, cryptographic evaluation or compliance with ISM, please contact DSD on (02) 62650197 or email assist@dsd.gov.au.

ACSI 33

The advice given in this document is in accordance with ISM release date September 2007. Australian Government agencies are reminded to periodically check the latest release of ISM at www.dsd.gov.au/library/infosec/acsi33.html.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 17 November 2008.